Why Unbreakable? ⇒ * Bit level shuffling

Page No. ②
Date

⊛ AES (Advanced Encryption Standard).

→ NIST - 2001
⇒ scandisk → FD
→ HD
Secure Access Program } AES 128-bit.

In our syllabus,

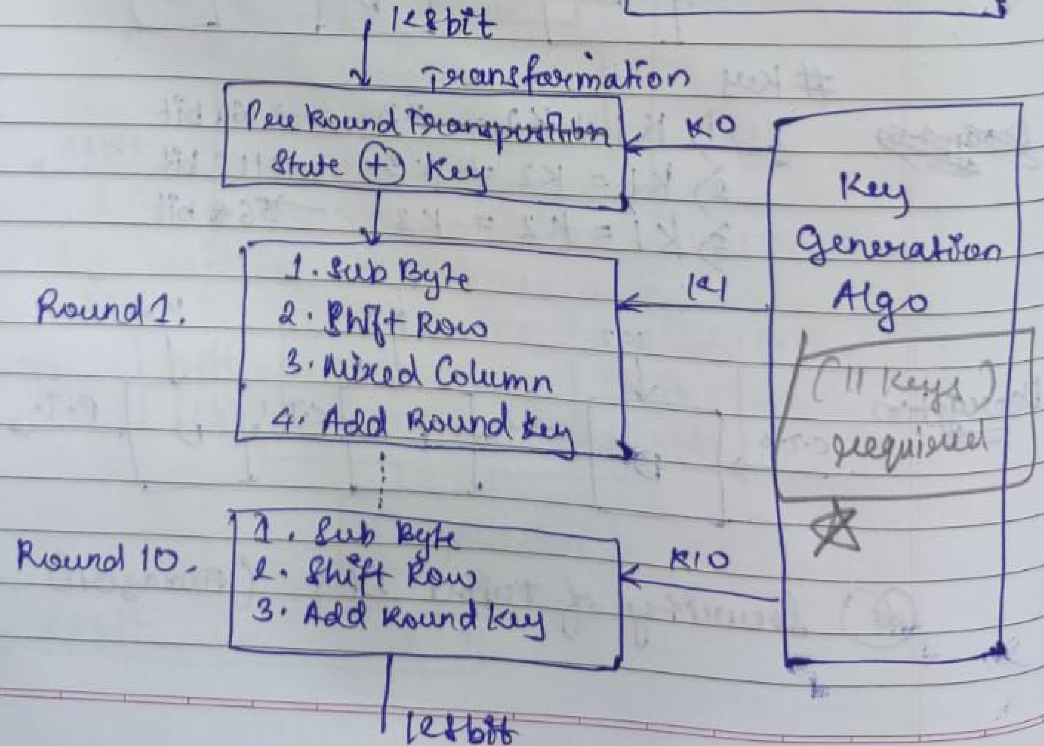
	Key Size	No. of Rounds
① AES - 128 bit	128 bit	10
② AES - 192 bit	192 bit	12
③ AES - 256 bit	256 bit	14

⇒ Lightweight algo. Used in mobile phone. Mixed Column Operation
⇒ If password lost, cannot be recovered.
→ Till now, AES is unbreakable (due to bit level shuffling)

⊛ AES - 128 bit.

Block Diagram of AES:

State:- 4x4 Matrix
16x8 = 128 bit



In Exam
For numerical 2x2
State:- UPPER CASE ONLY

(A) Pre Round Transformation.

$$\begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & \vdots & \vdots \\ a_2 & a_6 & \vdots & \vdots \\ a_3 & a_7 & . & a_{15} \end{bmatrix} \text{ State.}$$

Input => ABCDEF ..... OP

$$\begin{bmatrix} A & E & I & M \\ B & F & J & N \\ C & G & K & O \\ D & H & L & P \end{bmatrix}$$

Key => DJSANGHVICODECOMP.

$$\begin{bmatrix} D & N & I & C \\ J & G & C & O \\ S & H & O & M \\ A & V & E & P \end{bmatrix}$$

	Hex		Hex
A	00	N	0D
B	01	O	0E
C	02	P	0F
D	03	Q	10
E	04	R	11
F	05	S	12
G	06	T	13
H	07	U	14
I	08	V	15
J	09	W	16
K	0A	X	17
L	0B	Y	18
		Z	19

e),

s-bit

o. of Rounds
0
2
4

Mixed Column Operation
↓
level shuffling

4x4 Matrix
16x8 = 128 bit

Key Generation Algo
(11 Keys required)

State $\oplus$ Key

$A \oplus D$

Hexa

8-bit Binary

$00 \oplus 03$

$0000\ 0000 \oplus 0000\ 0011$

$= 0000\ 0011$

$= D.$

Key Expansion in AES 128bit Algo.

13/3/24

K_0 — $K_0(4\times4)$ Initial Key — K_1

$$\begin{array}{cccc} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ w_0 & w_1 & w_2 & w_3 \end{array} \longrightarrow \begin{array}{cccc} c_0 & c_4 & c_8 & c_{12} \\ c_1 & c_5 & c_9 & c_{13} \\ c_2 & c_6 & c_{10} & c_{14} \\ c_3 & c_7 & c_{11} & c_{15} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ w_4 & w_5 & w_6 & w_7 \end{array}$$

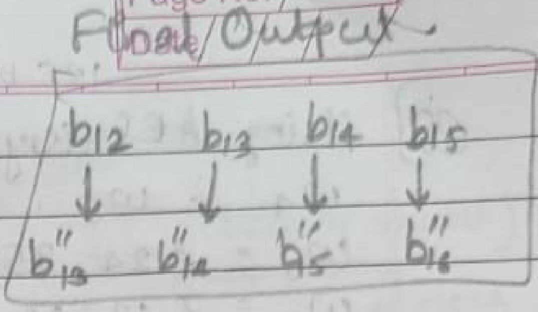
$$\boxed{w_4 = w_0 \oplus g(w_3)}$$

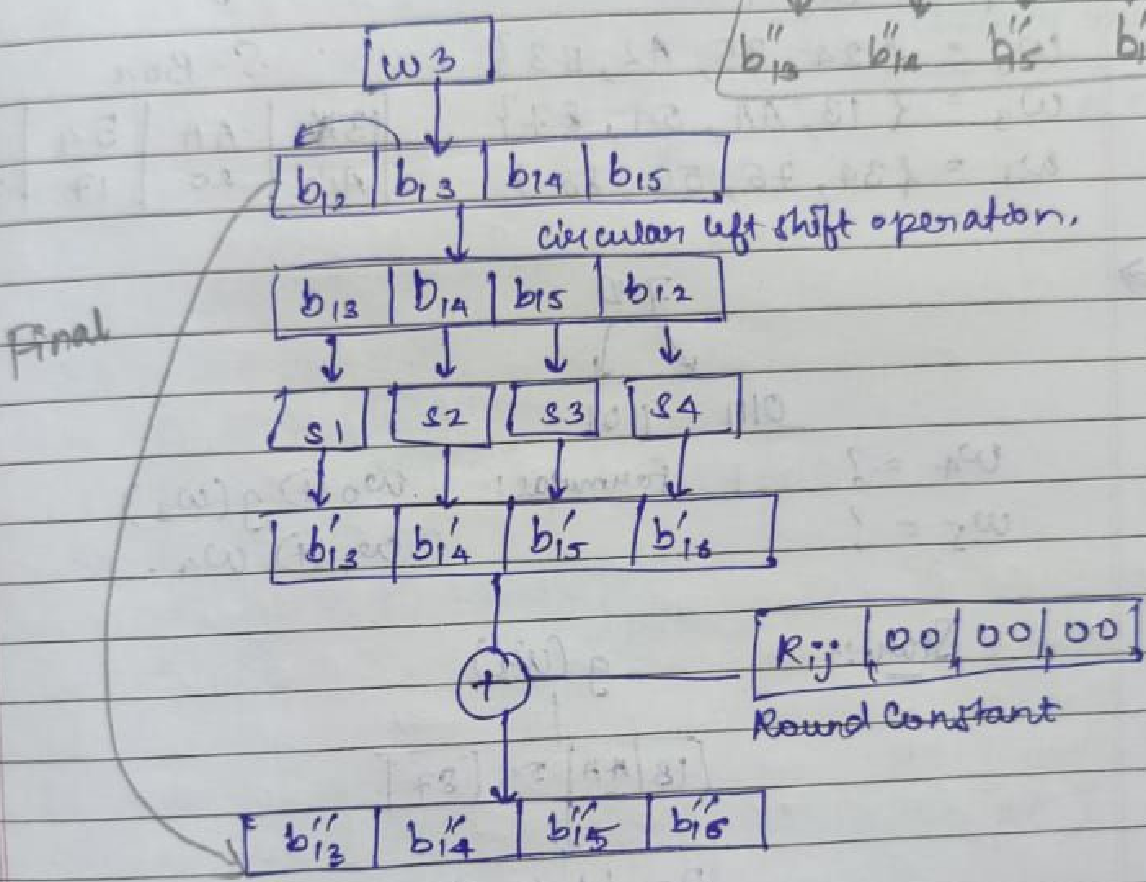
What happens.

$$w_5 = w_1 \oplus w_4$$
$$w_6 = w_2 \oplus w_5$$
$$w_7 = w_3 \oplus w_6$$

Page No.

$w_3 = \{b_{12}, b_{13}, b_{14}, b_{15}\}$





R_{ij} =

Round 1 = 01

2 = 02

3 = 04

4 = 08

5 = 10

⋮ ⋮

Round 10 = 36

$R_{ij} = x^{i-1}$ mod prime.

Page No. /
Date / /

(8 Ms)

Q] Using AES 128-bit Key Expansion technique generate w_4 & w_5.

$w_0 = \{24, 75, A2, B3\}$
$w_3 = \{13, AA, 54, 87\}$
$w_1 = \{34, 75, 56, 88\}$

S-Box

13	AA	54	87
AC	20	17	7D

⇒

7D → 0111 1101

$w_4 = ?$ formulae: $w_0 \oplus g(w_3)$
$w_5 = ?$ $w_1 \oplus w_4$.

Start:-

g(w_3)

13	AA	54	87

↓

Do 1 byte circular left shift

↓

AA	54	87	13

↓

S-Box

↓ (Given in Question)

20	17	7D	AC

$\oplus$

01	00	00	00

↓

x_1	x_2	x_3	x_4

1) Convert into binary
2) $\oplus$
3) Convert back to hexadecimal.

0	0	0
1	1	0
0	1	1
1	0	1

$$\begin{array}{r} 01 \\ \oplus\ 01 \\ \hline 00 \end{array} \qquad 01$$

Page No.
Date

$x_1 = 20 \oplus 01$
$= (\text{binary of } 20) \oplus (\text{binary of } 01)$ (Easy to convert)
$\quad \downarrow$ Hexa
$= 21$

$x_2 = 17 \oplus 00$
$= \text{binary} \oplus \text{binary}$
$\quad \downarrow$ Hexa
$= 17$

$x_3 = 7D \oplus 00$
$= \text{binary} \oplus \text{binary}$
$\quad \downarrow$ Hexa
$= 7D$

$x_4 = AC \oplus 00$
$= \text{binary} \oplus \text{Binary}$
$\quad \downarrow$ Hexa
$= AC$

$\therefore\ w_4 = w_0 + g(w_3)$
$= \{24, 75, A2, B3\} \oplus \{21, 17, 7D, AC\}$
$= \text{Binary} \oplus \text{Binary}$
$\quad \downarrow$ Hexa
$= \text{Hexa}$

Round 1 :- 1. Sub Byte
2. Shift Row
3. Mixed Column
4. Add Round Key

Page No.
Date 18/3/24

Sub Byte Operation

$$\begin{bmatrix} 2A & 3B \\ C1 & 12 \end{bmatrix}$$

State {2A, C1, 3B, 12}

S-Box

2A	C1	3B	12
D3	F1	14	15

⇒ Output:-

$$\begin{bmatrix} D3 & 14 \\ F1 & 15 \end{bmatrix}$$

{D3, F1, 14, 15}

Shift Row Operation

$$\begin{array}{l} 0^{th}\text{ row} \\ 1^{st}\text{ row} \\ 2^{nd}\text{ row} \\ 3^{rd}\text{ row} \end{array} \begin{bmatrix} 63 & 47 & a2 & F0 \\ F2 & 9c & 63 & 65 \\ Fb & ab & 7b & 7c \\ af & 76 & 76 & ca \end{bmatrix} \Rightarrow$$

After Shift Row

$$\begin{bmatrix} 63 & 47 & a2 & F0 \\ 9c & 63 & 65 & F2 \\ 7b & 7c & Fb & ab \\ ca & af & 76 & 76 \end{bmatrix} \begin{array}{l} \\ \{1\text{ byte LS}\} \\ \{2\text{ byte LS}\} \\ \{3\text{ byte LS}\} \end{array}$$

Mixed Column Operation. ☆ Bit Level Shuffling / Transposition ☆

State

$$\begin{bmatrix} x_0 & x_2 \\ x_1 & x_3 \end{bmatrix}$$

col 1 col 2

$$\begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \underbrace{\begin{bmatrix} C_0 & C_2 \\ C_1 & C_3 \end{bmatrix}}_{\text{Constant Matrix}} * \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}$$

⇒
$$b_0 = (C_0 * x_0) + (C_2 * x_1)$$
$$b_1 = (C_1 * x_0) + (C_3 * x_1)$$

Modulo Matrix Multiplication

(*) If in exam constant matrix not given, dont worry

It is PREDEFINED (*).

Page No. /
Date / / /

Constant Matrix. (4x4)

Constant Matrix 2x2

$$\begin{bmatrix} \boxed{\begin{matrix} 02 & 03 \\ 01 & 02 \end{matrix}} & \begin{matrix} 01 & 01 \\ 03 & 01 \end{matrix} \\ \begin{matrix} 01 & 01 \\ 03 & 01 \end{matrix} & \begin{matrix} 02 & 03 \\ 01 & 02 \end{matrix} \end{bmatrix}$$

1 byte RS (circular)
1 byte RS (circular)
1 byte RS (circular)

$s = \begin{bmatrix} 63 & 47 \\ f2 & 9c \end{bmatrix}$ $c = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix}$

$b = \begin{bmatrix} b_0 & b_2 \\ b_1 & b_3 \end{bmatrix}$ ← Output of col^n transposition.

→ $b_0 = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix} * \begin{bmatrix} 63 \\ f2 \end{bmatrix}$

$b_0 = (02 \underline{*} 63) + (03 \underline{*} f2) \cancel{+ (01 * 63) + (02 * f2)}$

$b_1 = (01 \underline{*} 63) + (02 \underline{*} f2)$

(*) Finite Field Arithmetic Operation
- $GF(2^8)$ → Gallium Field.
- → Max shuffling of data/info will be carried out by $GF(2^8)$

In ~~ad~~ AES, multiplication ~~is performed~~ of 2 hexadecimal values is performed by using FFAO i.e. $GF(2^8)$

This FFAO is supporting maximum scrambling of data.

$b_0 = (02 * 63) \oplus (03 * f2)$

$02 = 0000 \quad 0010$
$63 = 0110 \quad 0011$

$GF(2^8) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$GF(2^8) = \{0000 \ 0000 \ \cdots\cdots \ 1111 \ 1111\}$

$\{02\} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0$
$= x$

$\{63\} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$= 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1$
$= x^6 + x^5 + x + 1$

$\therefore \ 02 * 63$
$= x * (x^6 + x^5 + x + 1)$
$= x^7 + x^6 + x^2 + x$

$\therefore$ Now,

x^7	x^6	x^5	x^4	x^3	x^2	x	1
1	1	0	0	0	1	1	0

$= 1100 \ 0110$
$= C6$

$03 = 0000 \quad 0011$

$f2 = 1111 \quad 0010$

$\{03\} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$= 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1$

$= x + 1$

$\{f2\} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$= 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0$

$= x^7 + x^6 + x^5 + x^4 + x$

$\therefore \quad 03 * f2$

$= (x+1) * (x^7 + x^6 + x^5 + x^4 + x)$

$= x^8 + x^7 + x^6 + x^5 + x^2 + x^7 + x^6 + x^5 + x^4 + x$

$\cancel{= x^8 + 2x^7 + 2x^6 + 2x^5 + x^4 + x^2 + x}$.

Ex-OR,

$x^8 \oplus \cancel{x^7} \oplus \cancel{x^6} \oplus \cancel{x^5} \oplus x^2 \oplus \cancel{x^7} \oplus \cancel{x^6} \oplus \cancel{x^5} \oplus x^4 \oplus x$

$= x^8 + x^4 + x^2 + x$.

The degree of above polynomial is 8 which is not part of GF (2^8). Maximum degree supported by GF (2^8) is 7. We need to convert above polynomial into reduced poly. We need to convert above polynomial by irreducible poly. For that purpose, ÷ above polynomial by irreducible poly.

Irreducible Polynomial:

$P(x) = x^8 + x^4 + x^3 + x + 1$

$= 100011011$

Page No. / Date

$G(x) = x^8 + x^4 + x^2 + x$

~~P(x) = 10001~~

$P(x) = x^8 + x^4 + x^3 + x + 1$

$\therefore t(x) = G(x) / P(x)$

~~= 1000101110~~

	1
100011011	1 0 0 0 1 0 1 1 0
	⊕ 1 0 0 0 1 1 0 1 1
	0 $\boxed{0\ 0\ 0\ 0}$ $\boxed{1\ 1\ 0\ 1}$

$= 0D$

$\therefore (03 * F2) = 0D$

$b_0 = (02 * 63) \oplus (03 * F2)$

$= C6 \oplus 0D$

$=$

$$\begin{array}{r} 1\,1\,0\,0 \quad 0\,1\,1\,0 \\ \oplus\ 0\,0\,0\,0 \quad 1\,1\,0\,1 \\ \hline 1\,1\,0\,0 \quad 1\,0\,1\,1 \end{array}$$

$b_0 = CB$

Page No.
Date

$b_1 = \underbrace{(01 * 63)}$ $\oplus$ $\underbrace{(02 * f2)}$

$01 = 0000 \quad 0001$
$63 = 0110 \quad 0011$

$GF(2^8) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\{01\} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\quad\quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1$
$= 1.$

$\{63\} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$= 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1$
$= x^6 + x^5 + x + 1.$

$01 * 63$
$= 1 * (x^6 + x^5 + x + 1)$
$= x^6 + x^5 + x + 1$

Now,
$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1$

$= \underbrace{0110}_{6},\ \underbrace{0011}_{3},$
$= 6 \quad 3$

Page No.
Date

$02 = 0000 \quad 0010$
$f2 = 1111 \quad 0010$

$\{02\} = x$
$\{f2\} = x^7 + x^6 + x^5 + x^4 + x$

$02 * f2$
$= x * (x^7 + x^6 + x^5 + x^4 + x)$
$= x^8 + x^7 + x^6 + x^5 + x^2$

Now,

Pre defined

$G(x) = x^8 + x^7 + x^6 + x^5 + x^2$
$\boxed{P(x) = x^8 + x^4 + x^3 + x + 1}$

$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

1 1 1 1 0 0 1 0 0

1 0 0 0 1 1 0 1 1

$t(x) = G(x) / P(x)$

100011011 | 1
111100100
⊕ 100011011
011111111

$= \underbrace{1111}_{F}\underbrace{1111}_{F}$
$= F \; F$

Page No.
Date

$b_1 = (01 * 63) \oplus (02 * f2)$
$= 63 \oplus FF$

$= 0110 \quad 0011$
$\oplus 1111 \quad 1111$

$\underbrace{1001}$ $\underbrace{1100}$ binary to hexadecimal

$b_1 = 9c$

$$\begin{bmatrix} b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix} * \begin{bmatrix} 47 \\ 9c \end{bmatrix}$$

$b_2 = (02 * 47) \oplus (63 * 9c)$
$b_3 = (01 * 47) \oplus (02 * 9c)$

$b_2 = (02 * 47) \oplus (63 * 9c)$

Threat → Man in Middle *

Not Encryption/Decryption

Objective → Key Exchange

* Diffie-Hellman Algo.

Process to find out primitive root of prime number.

$p = 7$

$2^1 \bmod 7 = 2$
$2^2 \bmod 7 = 4$
$2^3 \bmod 7 = 1$ Repeating.
$2^4 \bmod 7 = 2$
⋮
$\therefore$ ② ✗
$(1 \ldots (p-1))$
Power $\therefore$ $(1 \ldots 6)$

$3^1 \bmod 7 = 3$
$3^2 \bmod 7 = 2$
$3^3 \bmod 7 = 6$
$3^4 \bmod 7 = 4$
$3^5 \bmod 7 = 5$
$3^6 \bmod 7 = 1$ ✓

$\alpha = 3$

Sender	Receiver.
① Select Prime no "P." α → Primitive Root of P $\xrightarrow{P,\ \alpha}$	
② Find out private Key $= (X_A)$ # Random number	② Find out Private Key (X_B) # Random number.
③ Find out public key $Y_A = (\alpha)^{X_A} \bmod p$	③ Find out public Key $Y_B = (\alpha)^{X_B} \bmod p$
④	④
$\xleftarrow{Y_b}$	$\xrightarrow{Y_a}$
⑤ Secret key Calculation $Y_1 = (Y_b)^{X_A} \bmod P$ ↳ Public Key of Receiver.	⑤ Secret Key Calculation $Y_2 = (Y_a)^{X_B} \bmod P$ ↳ Public Key of Sender

$\boxed{Y_1 == Y_2}$

$P = 11$ · Find α.

Find Private, Public, ~~Seck~~ Secret Key.

$\Rightarrow$ $P = 11$

$2^1 \bmod 11 = 2$ $\quad$ $2^6 \bmod 11 = 9$

$2^2 \bmod 11 = 4$ $\quad$ $2^7 \bmod 11 = 7$

$2^3 \bmod 11 = 8$ $\quad$ $2^8 \bmod 11 = 3$

$2^4 \bmod 11 = 5$ $\quad$ $2^9 \bmod 11 = 6$

$2^5 \bmod 11 = 10$ $\quad$ $2^{10} \bmod 11 = 1$

$\alpha = 2$ ✓

Now, $X_A = 3$ $\quad$ $X_B = 5$

$\therefore y_A = (\alpha)^{X_A} \bmod P$ $\quad$ $y_B = (\alpha)^{X_B} \bmod P$

$= (2)^3 \bmod 11$ $\quad$ $= (2)^5 \bmod 11$

$y_A = 8$ $\quad$ $y_B = 10$

Now Exchange.

$y_1 = (10)^3 \bmod 11$ $\quad$ $y_2 = (8)^5 \bmod 11$

$y_1 = 10$ $\quad$ $y_2 = 10$

$y_1 == y_2$

Private Key = 3, 5

Public Key = 8, 10

Secret Key = 10

$(2)^{13} \bmod 11$ $\quad$ $(2)^{15} \bmod 11$

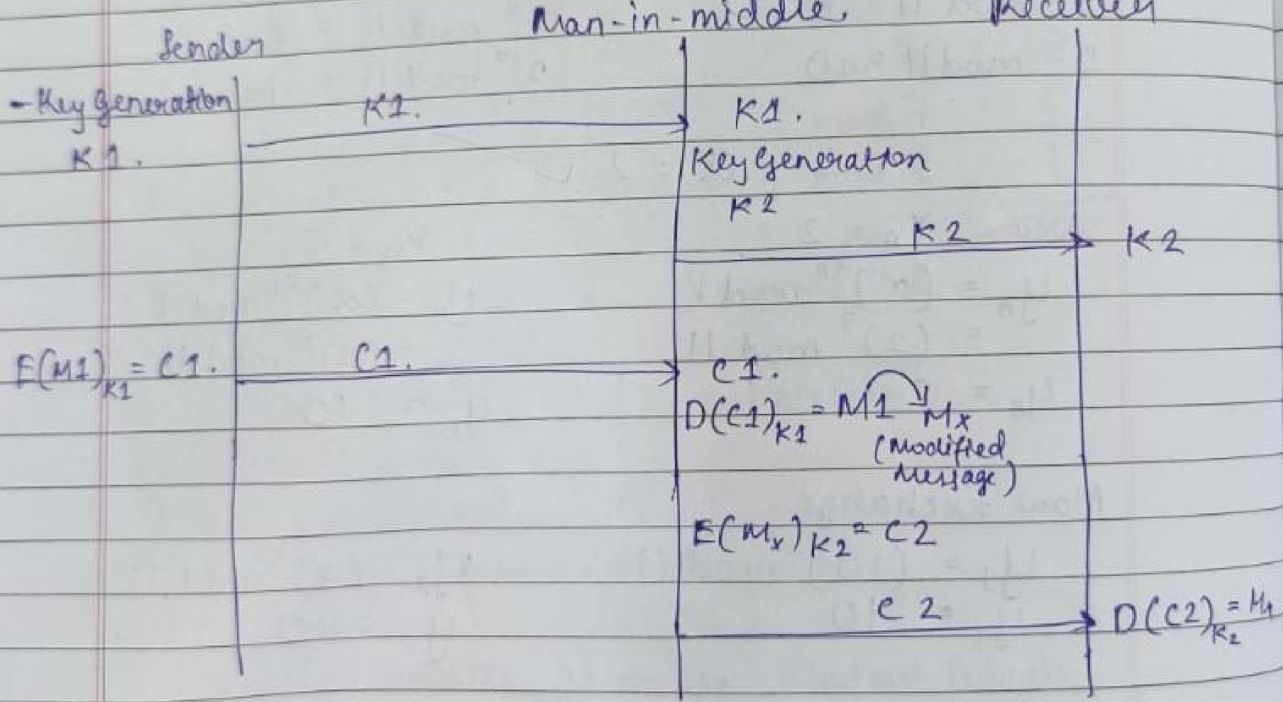
Page No.
Date 8/4/24

Man-in-Midde Attack.

During Key Exchange.

Man-in-middle attack on

(a) Symmetric Key Exchange Algo.



(b) Asymmetric Key Exchange Algo.

[Objective of communication : Sender wants to transfer message (M1) to Receiver in secured manner.

Receiver will generate the public key & private key using RSA algorithm.]

$Kx_1 = (y_B)^{x_{A_1}} \bmod P$

← Asix.

Page No.
Date

Sender | Man-in-middle | Receiver.

(M1)

Req for Receiver for Public Key →

Req for Ker. for Public Key →

RSA → K1, K2

K1 = Public
K2 = Private

← K1

K1.
RSA → Kx_1 Public, Kx_2 Private

Kx_1 ← Kx_1 → Public key of Man-in-middle.

$E(M1)_{Kx_1} = C1$

C1 →

$D(C1)_{Kx_2} = M1.$ → M_x

$E(M_x)_{K1} = C2$

C2 →

$D(C2)_{K2} = M_x.$

Flair GLASS GEL

(c) Diffie - Hellman Algo.

Sender | Man-in-middle. | Receiver.

P, α → P, α → P, α

X_B → Private Key.

$y_B = (\alpha)^{x_B} \bmod P.$

X_A → Private Key

$y_A = (\alpha)^{x_A} \bmod P$

y_A →

← y_B

Hacker has (y_A, y_B) →

x_{A_1}, x_{B_1} → Private Key

$y_{A_1} = (\alpha)^{x_{A_1}} \bmod P$

$y_{B_1} = (\alpha)^{x_{B_1}} \bmod P$

Public Key

← y_{B_1}

y_{A1} →

Secret Key
$K1 = (y_{B_1})^{X_A} \bmod P$

$K2 = (y_{A_1})^{X_B} \bmod P.$

Kx_1 ?

$K_{x_1} \longleftrightarrow K_1$

&

$K_{x_2} \longleftrightarrow K_2$

$\therefore K_{x_1} = (y_B)^{x_{A_1}} \bmod P$

$K_{x_2} = (y_A)^{x_{B_1}} \bmod P$

\# $P = 11$, $\alpha = 7$. Public keys of Sender & Receiver.

Private keys of sender & Reciever $x_A = 3$, $x_B = 9$ $\quad y_A = ?$ $\quad y_B = ?$

Hacker: $x_{A_1} = 8$, $x_{B_1} = 6$. $\quad y_{A1} = ?$ $\quad y_{B1} = ?$

Secret keys: $K1 = ?$, $K2 = ?$, $Kx_1 = ?$, $Kx_2 = ?$.

$$\Rightarrow \quad y_{A1} = (\alpha)^{x_{A1}} \bmod P = (7)^8 \bmod 11 = 9$$

$$y_{B1} = (\alpha)^{x_{B1}} \bmod P = (7)^6 \bmod 11 = 4$$

$$K1 = (y_{B1})^{x_A} \bmod P = (4)^3 \bmod 11 = 9$$

$$K2 = (y_{A1})^{x_B} \bmod P = (9)^9 \bmod 11 = 5$$

438800 3681509

Page No. 25201
Date / / /

$$\boxed{K_{x_1} = (y_B)^{x_{A_1}} \bmod P}$$

$\cancel{7}$

$$\therefore y_B = (\alpha)^{x_B} \bmod 11$$
$$= (7)^9 \bmod 11$$
$$= 8$$

$$K_{x_1} = (8)^8 \bmod 11$$
$$\boxed{K_{x_1} = 5}$$

$$\boxed{K_{x_2} = (y_A)^{x_{B_1}} \bmod P}$$

$\cancel{7}$

$$\therefore y_A = (\alpha)^{x_A} \bmod 11$$
$$= (7)^3 \bmod 11$$
$$= 13$$

$$\therefore K_{x_2} = (13)^6 \bmod 11$$
$$\boxed{K_{x_2} = 9}$$

Ulta aa gaya.

Ans should be: $K_1 == K_{x_1}$
$K_2 == K_{x_2}$

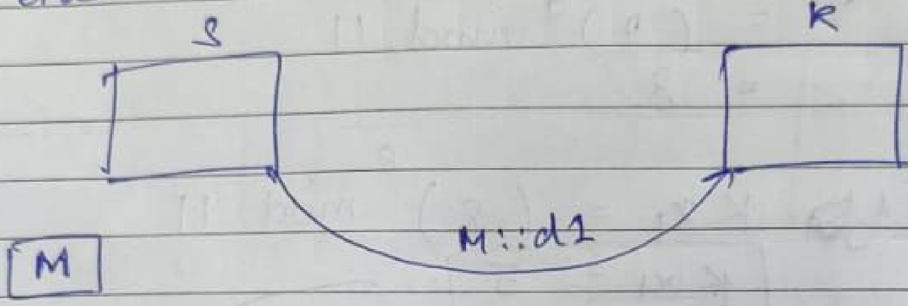
Correct:

$$\boxed{\begin{aligned} K_{x_1} &= (y_A)^{x_{B_1}} \bmod P \\ K_{x_2} &= (y_B)^{x_{A_1}} \bmod P \end{aligned}}$$

106.95

Integrity.

Various hashing algo re used to Msg. Below diagram is representing how integrity of msg is verified at receiving end.



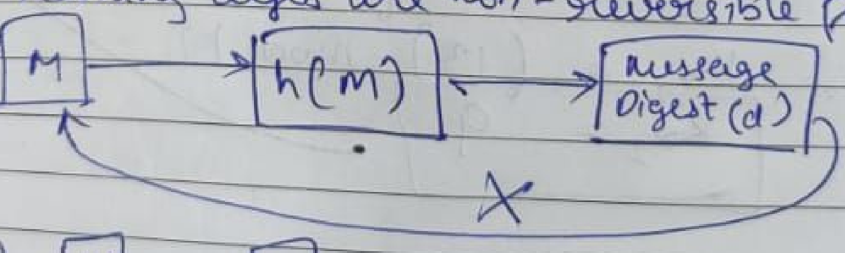
(1) h(M) = d1 (Message Digest) h(M) = d2

(2) M → Message. d2 - d1 = 0

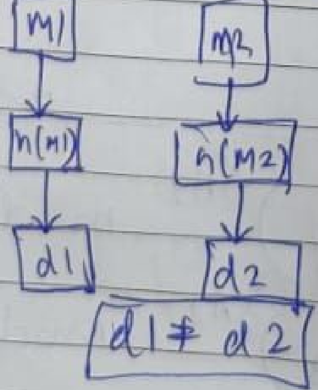
Hashing Technique

Hashing Properties:

(i) Hashing algos are non-reversible function.



(ii)



No collision should be there.

Hashing Algorithm Properties

Self Study.

Page No. / Date

(*) Message Digest (MD)
- Ron Rivest
- MD, MD2, MD3, MD4, MD5.

MD5-Algorithm:

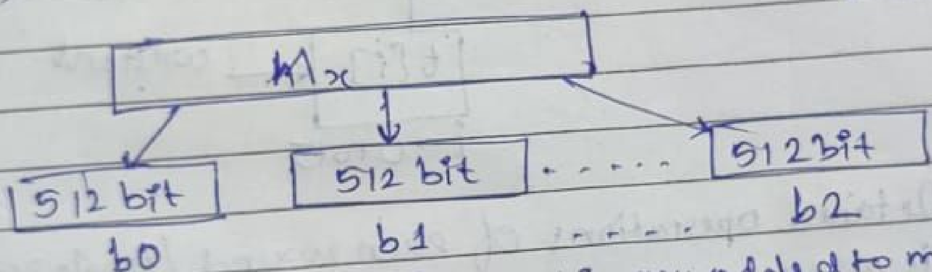
(i) Calculate length of Message. (l)

(ii) Add length to the original message. (m+L)

(iii) Divide message into 512 bit blocks.

$\leftarrow M_x \rightarrow$

M	L



(iv) Padding. (Extra bits are added to make sure all blocks are 512 bits.)

~~(v) Divide 512 bit blocks into 16~~

(v) Initial chaining variable → Inducing Randomness, Increases strength.

a, b, c, d

Size of each chaining variable is 32-bit. → hexadecimal value.

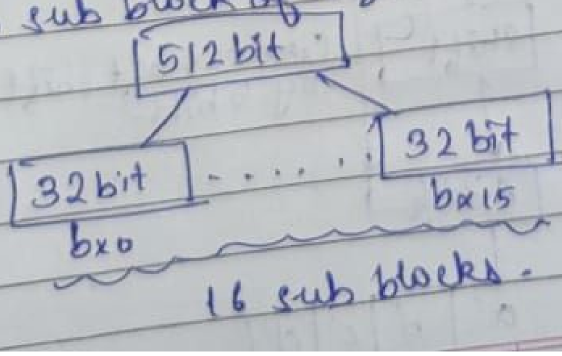
Eg:-
a=
01 23 45 67

(vi) Copy chaining variable into another temp variables.

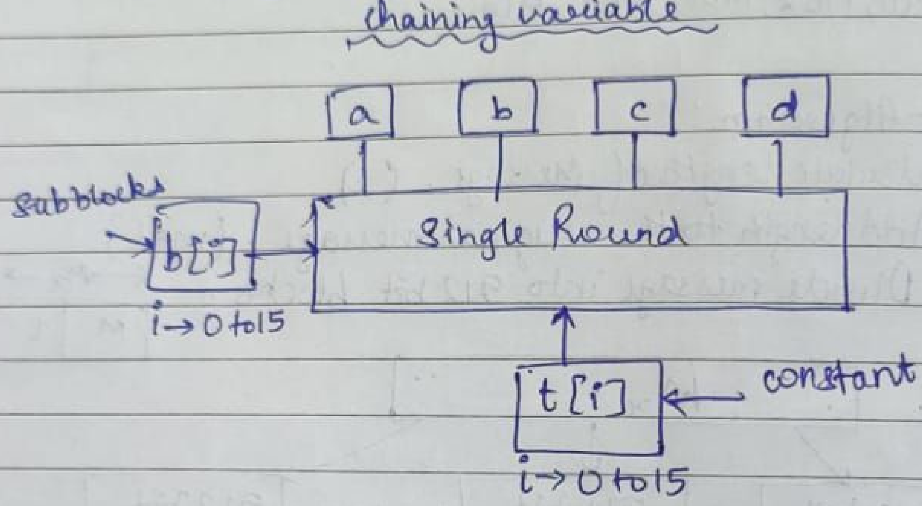
a	b	c	d
a'	b'	c'	d'

→ chaining variable
→ Temp. chaining variable.

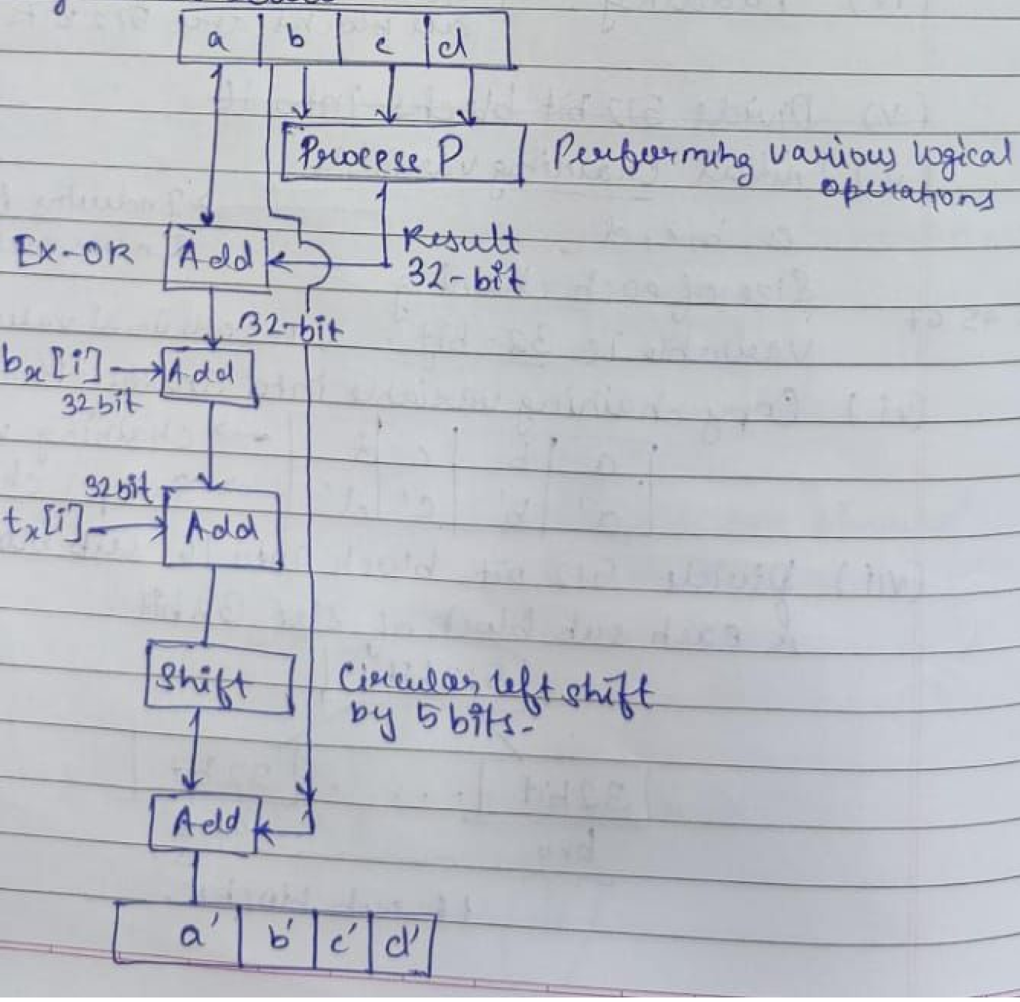
(vii) Divide 512 bit block into 16 sub block & each sub block of size 32 bit.



(viii) MD5 Algo is performing 4 Round off operation.
Block dig. of each Round is given as below



(ix) Detailed operations of each round / single round is given as below



The limitation / drawbacks of MD5 algorithm is only single chaining variable is being modified during each operation.